REMARKS/ARGUMENTS

This Response to Office Action, which is filed with an accompanying REQUEST FOR CONTINUED PROSECUTION, is responsive to the Office Action from the Examiner mailed September 20, 2005. Reconsideration and withdrawal of the rejections set forth in the Office Action is respectfully requested. The applicants have amended claims 1, 3, 10, 12, 19, 25, and 31-44. No new matter has been added. Claims 1-3, 10-12, 19, 25 and 31-44 are pending in this application.

This Response and the accompanying REQUEST FOR CONTINUED PROSECUTION are filed within six months of the mailing date of the FINAL REJECTION.

The applicants respectfully disagree with the Examiner's Response to Arguments, but have amended the claims to bring this application to issuance. The applicants reserve the right to reintroduce the original claims in a later Office Action response, or in a continuation.

The Rejections

The Examiner rejected claims 1-3, 10-12, 19, 25, 31, and 32 under 35 U.S.C. 102(e) as anticipated by U.S. Pat. No. 6,810,525 (Safadi et al.). The Examiner rejected claims 1-3, 10-12, 19, 25, and 31-44 under 35 U.S.C. 102(e) as anticipated by U.S. Pat. No. 6,775,779 (England et al.).

The Prior Art (Safadi et al.)

Safadi et al. apparently disclose a method and system for impulse purchasing of services over a communication network. Safadi et al. disclose an access controller which generates an encrypted message in response to an IPPU selection (Col. 1, lines 62-66). The encrypted message is then sent to the subscriber terminal to verify if the IPPU selection is within a credit entitlement of the subscriber (Col. 1 lines 67 – Col. 2 lines 7). If the subscriber has sufficient credit, then the client application will "send the entitlement token to a server (e.g., a proxy/policy server) in a secure manner in order to

determine the status of the subscriber's entitlement to receive the IPPU selection. If the subscriber's entitlement to receive the IPPU selection is verified, the server will further process the IPPU selection for further enabling the selected service/application for use by the viewer" (Col. 2, lines 11-18).

As is well-known in the relevant art, a network filesystem is a client/server application that lets a computer user view and optionally store and update file on a remote computer as though they were on the user's own computer. This is critically important in some streaming software applications, since streaming-enabled applications on a client computer may spoof a filesystem, tricking the filesystem into acting like the streamable application is stored locally, even though some or all of the streaming-enabled program files are stored remotely.

Safadi et al. do not explicitly disclose a network filesystem, and a network filesystem is not necessary for the Safadi et al. invention to operate properly. Notably, Safadi et al. do not disclose streaming software applications, either.

The Prior Art Distinguished (Safadi et al.)

Claim 1 includes the language: "said network filesystem handles and forwards requests from steaming-enabled local processes on said client that are directed at streaming application program files located on said server..." Since Safadi et al. do not disclose streaming-enabled local processes, it follows that Safadi et al. do not teach a network filesystem that handles requests for streaming application program files on a server.

Claim 1 also includes the language: "said network redirector component makes visible to said network filesystem, a path that represents the server where said streaming application program files are stored." Safadi et al. do not disclose making a path visible to a network filesystem, and have no obvious reason to do so.

To anticipate a claim, the prior art reference must teach every element of the claim. MPEP 2131. Since Safadi et al. do not teach every element of Claim 1, Claim 1 is

allowable over Safadi et al. Claims 2-3, which depend from claim 1, are allowable at least for depending from an allowable independent claim.

Claims 10-12, 19, 25, and 31-44 are allowable for reasons similar to those described with reference to claim 1.

The Prior Art (England et al.)

England et al. apparently disclose: An architecture for protecting premium content in a nonsecure computer environment executes only a small number of code modules in a secure memory. The modules are arranged in a hierarchy of trust, where a module names other modules that it is willing to trust, and those modules in turn name other modules that they are willing to trust. A secure loader loads a security manager that oversees a number of content-providing modules for manipulating the content. A memory manager assigns permissions to various pages of the secure memory. The memory has rings of different security. The security model can be extended to program modules and other devices on the computer's bus, such as DMA controllers and peripherals.

Notably, England et al. do not disclose streaming software.

The Prior Art Distinguished (England et al.)

Since England et al. do not disclose streaming software, the pending claims are allowable over England et al. for reasons similar to those described with reference to the Safadi et al. reference.

Conclusion

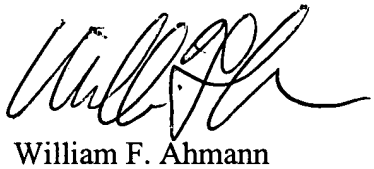
In view of the foregoing, Applicants submit that all the claims pending in the application patentably define over the prior art. The Applicants respectfully requests the Examiner withdraw rejections of all claims. A Notice of Allowance is respectfully requested.

If extra fees are due, please charge our Deposit Account No. 50-0665 from which the undersigned is authorized to draw.

If in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call the undersigned at (650) 838-4305.

Respectfully Submitted,

PERKINS COIE LLP



Date: December 19, 2005

William F. Ahmann

Reg. No. 52,548

Correspondence Address:
Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 94026
650-838-4300